

Fig. 1(a)

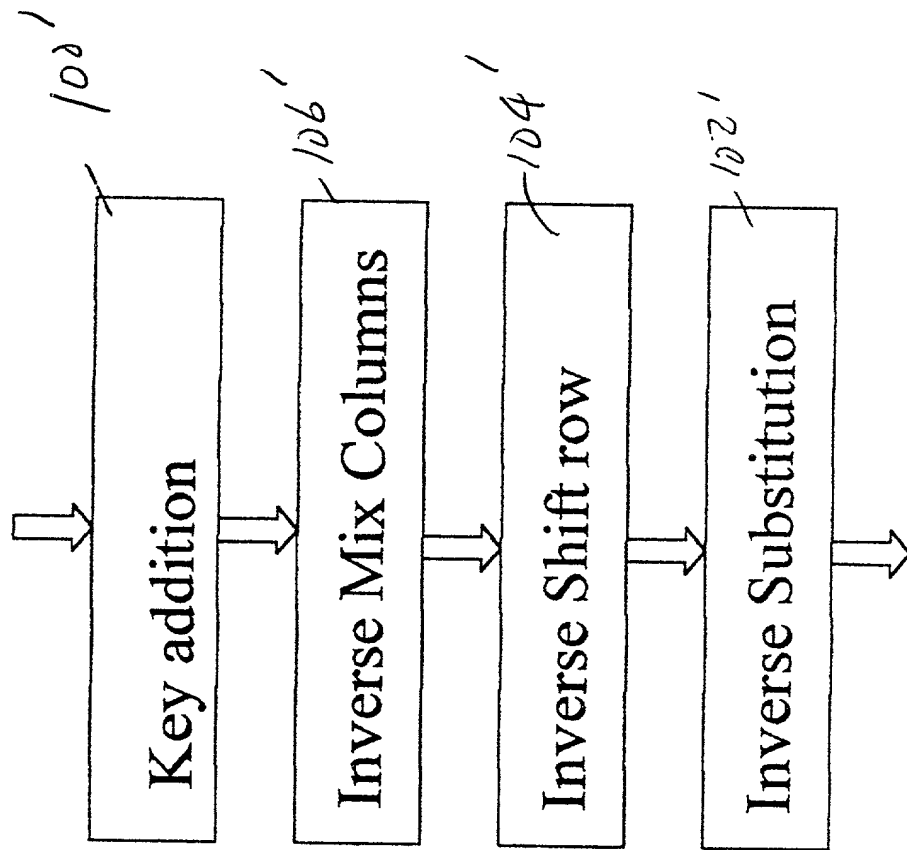


Figure 1(b)

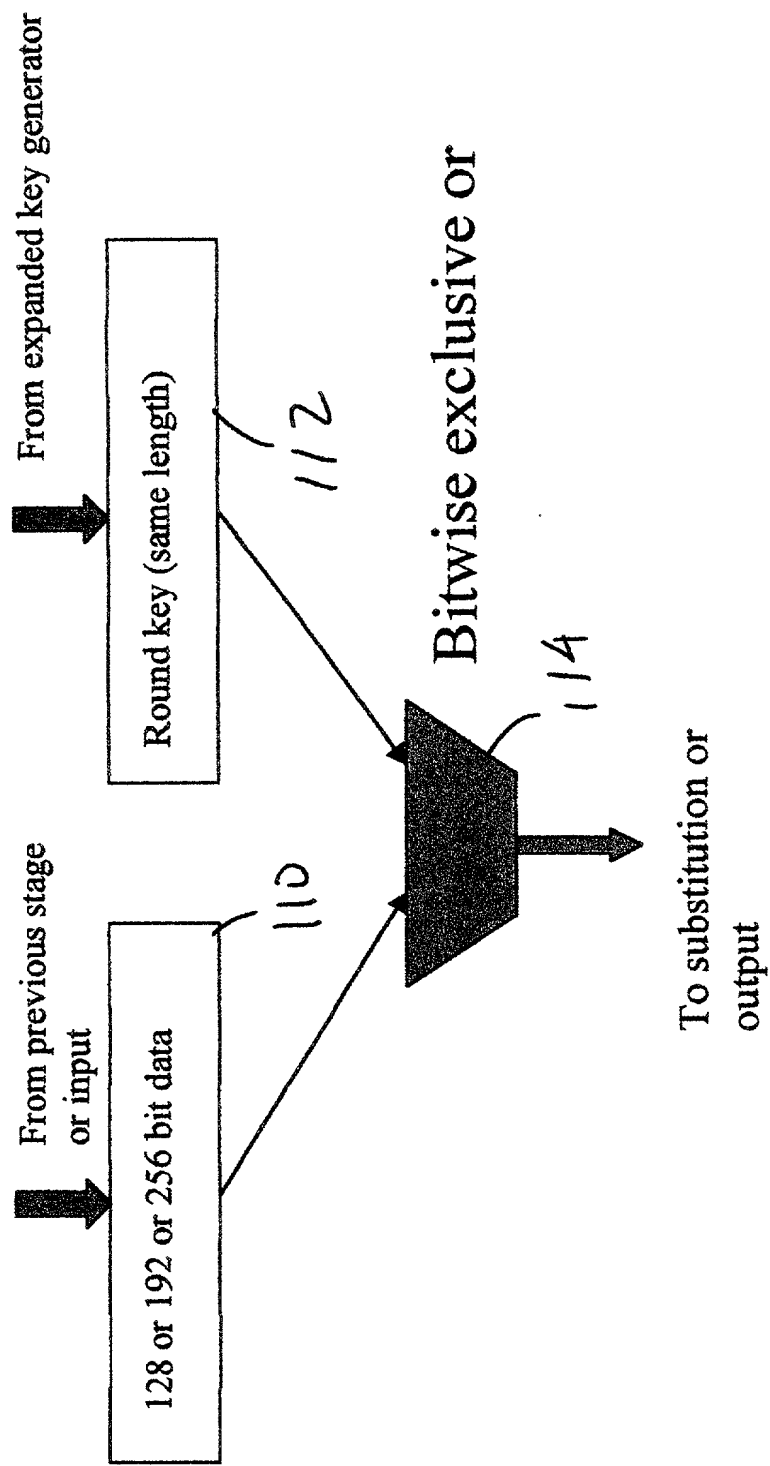


Fig. 2

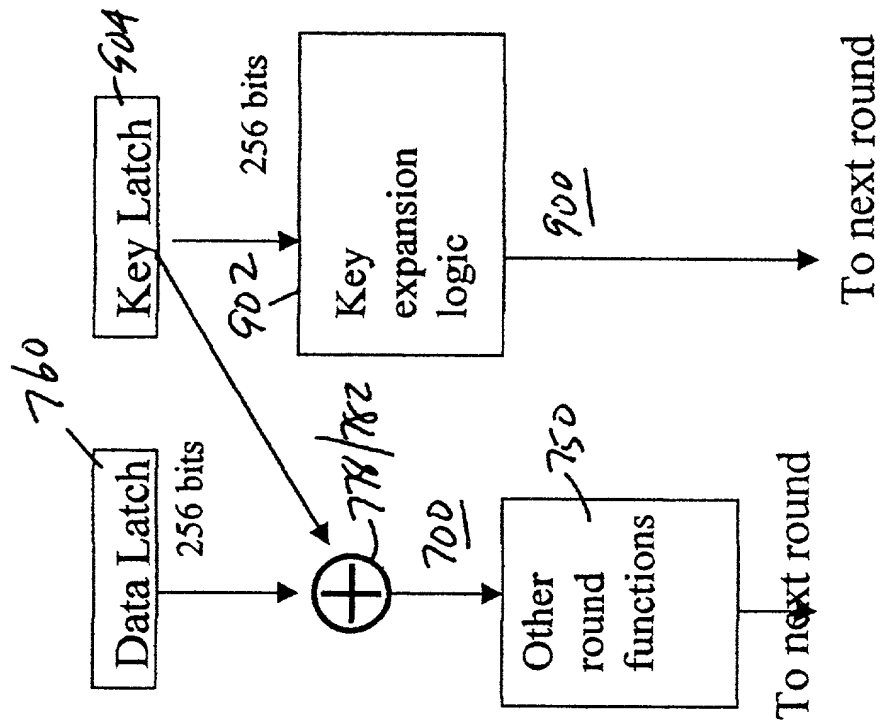


Fig. 39

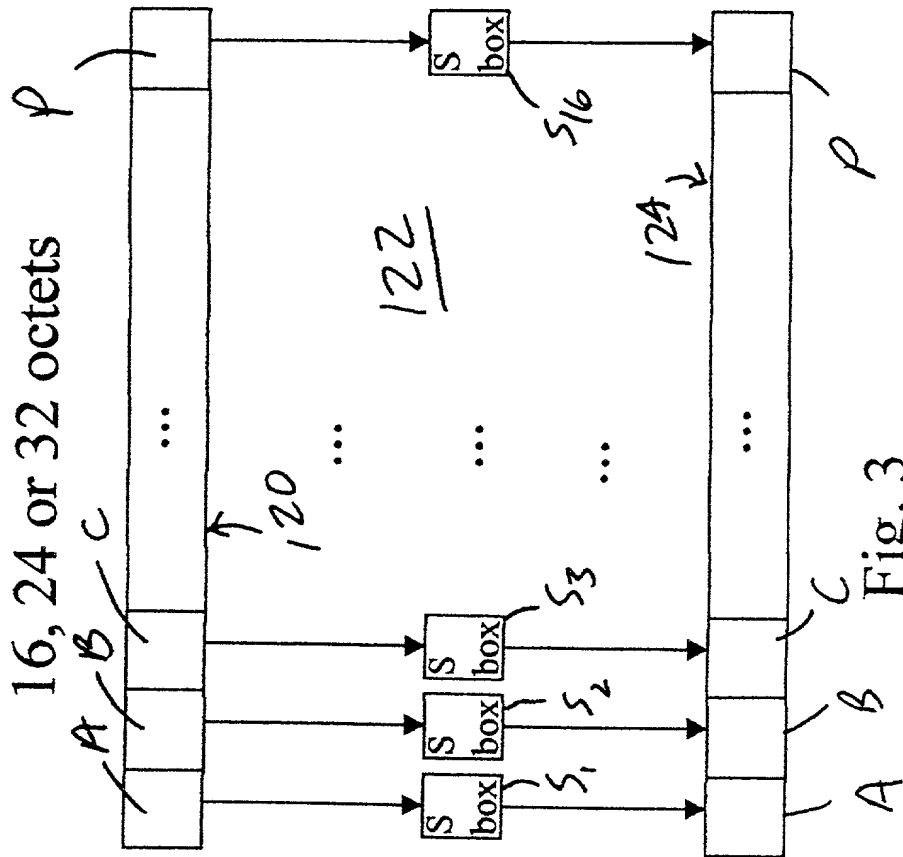


Fig. 3

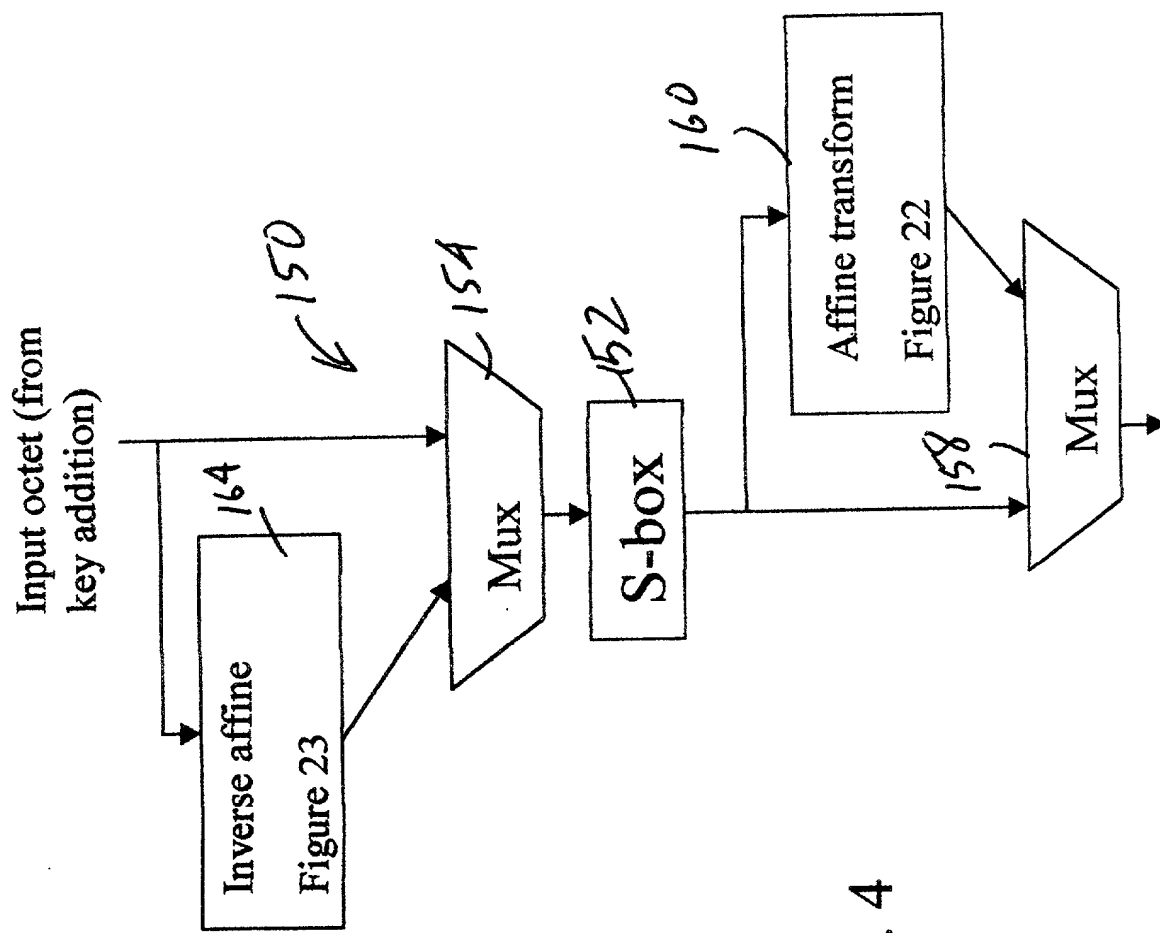
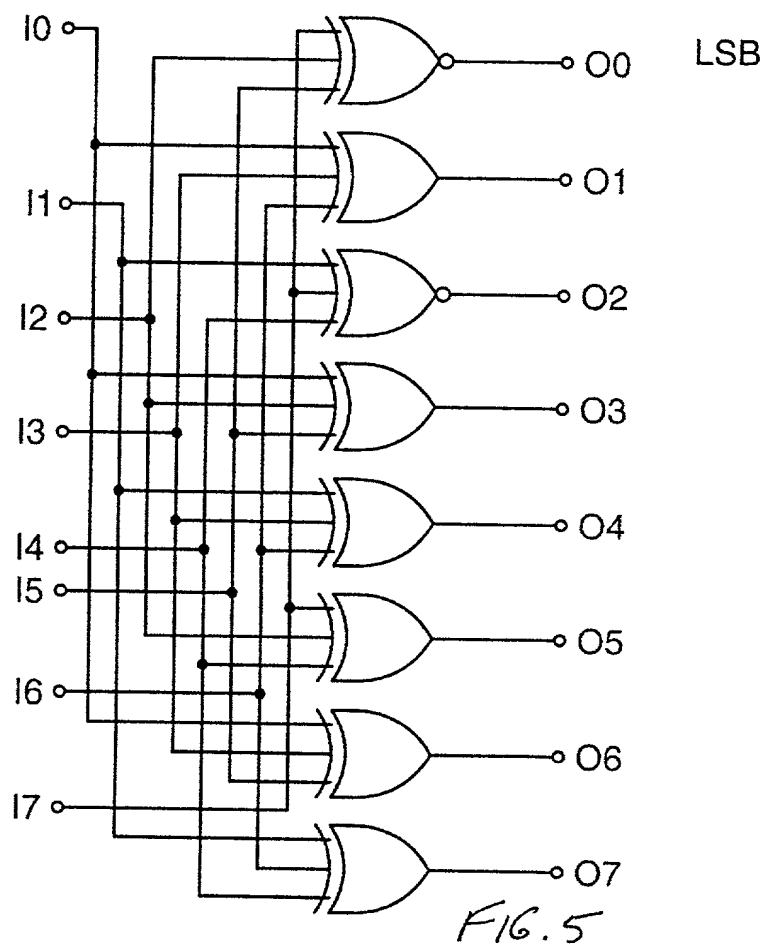
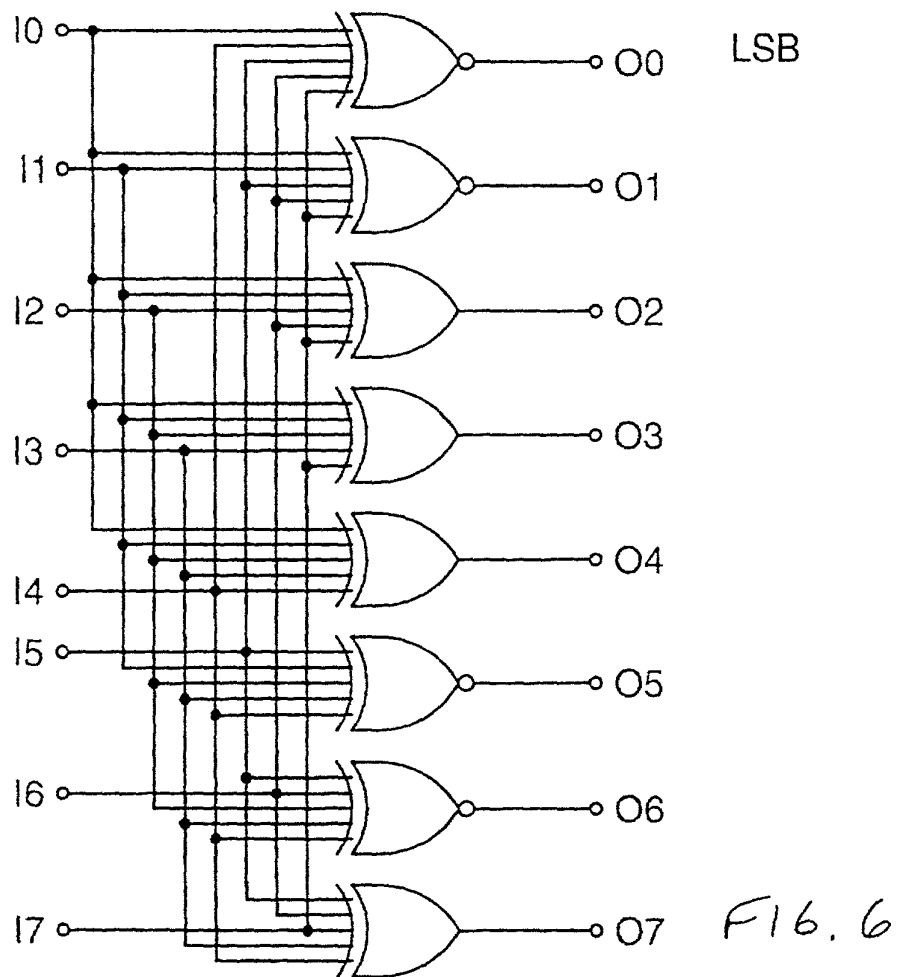


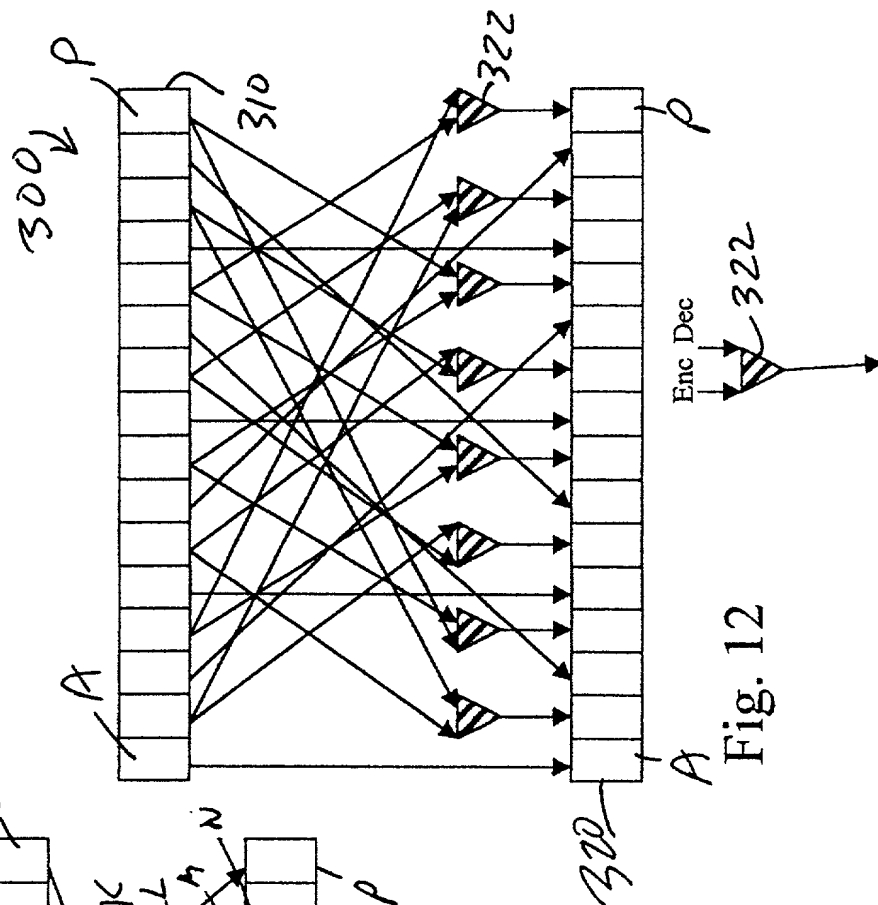
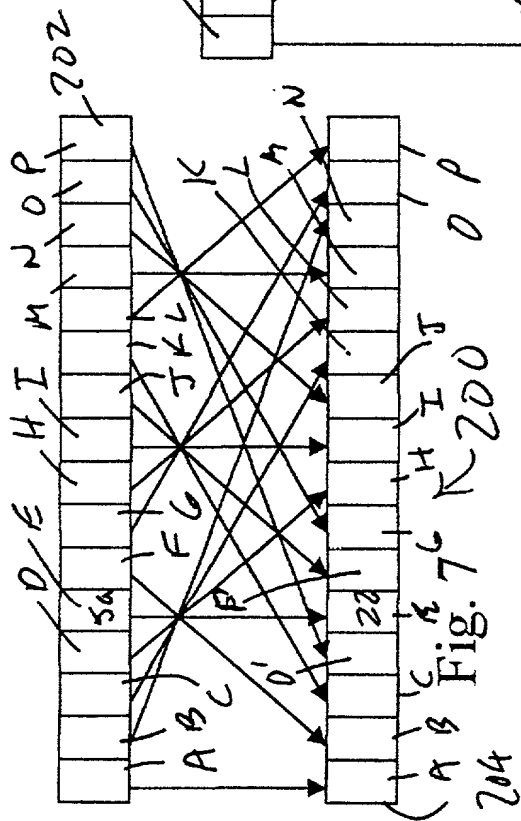
Fig. 4

Inverse Affine transform, decryption S-Box pre-processing



Affine transform, encryption S-Box post processing





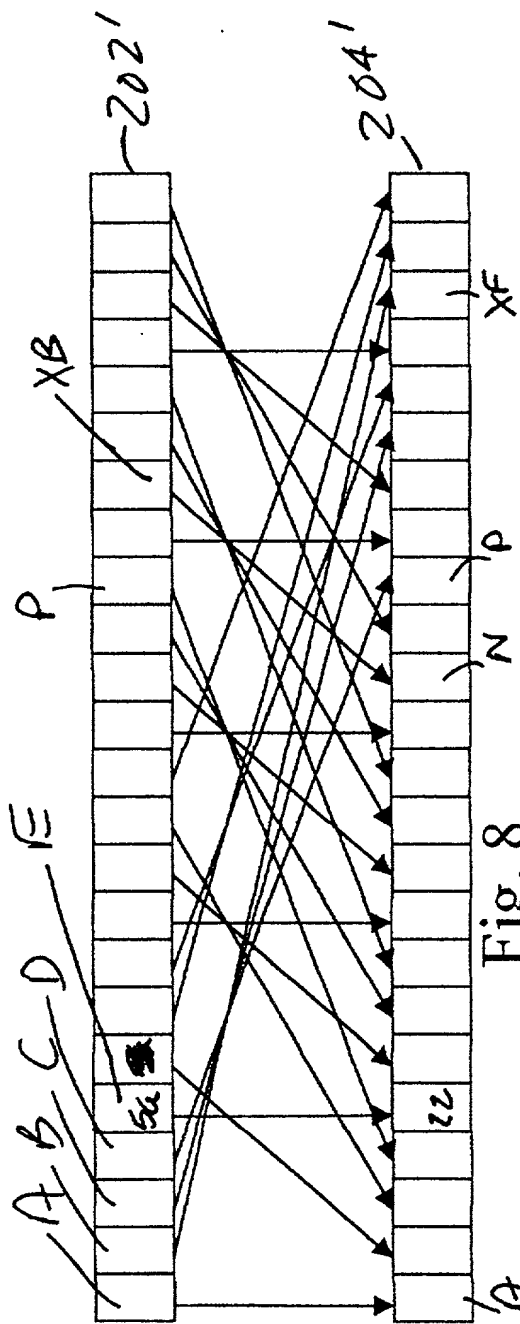


Fig. 8

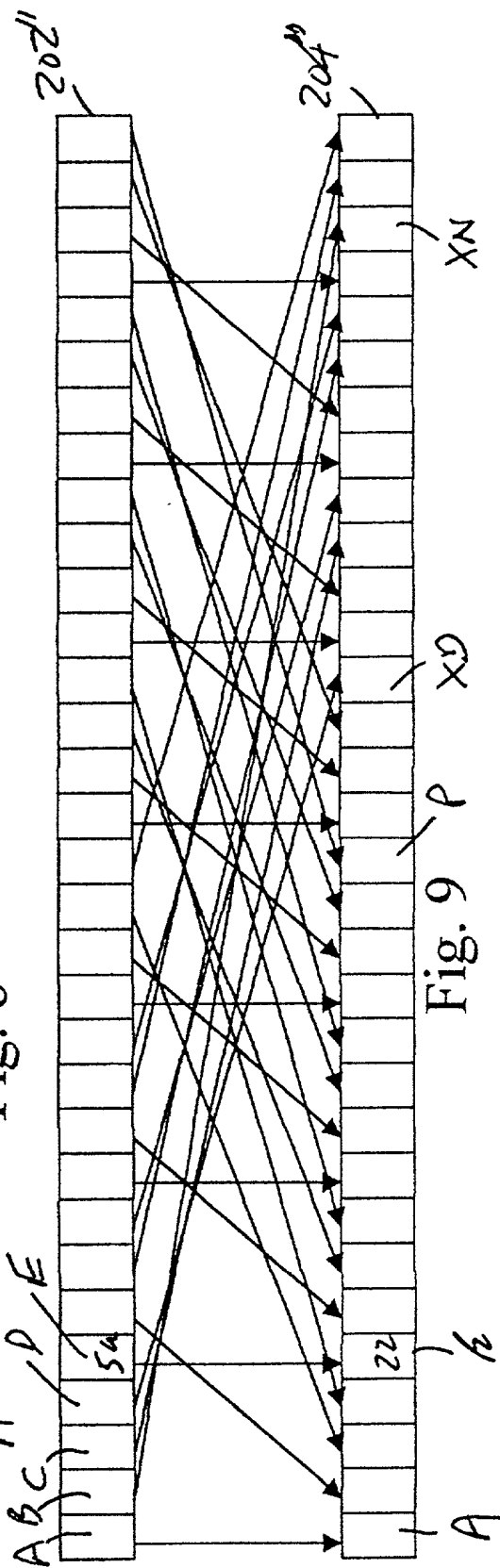


Fig. 9

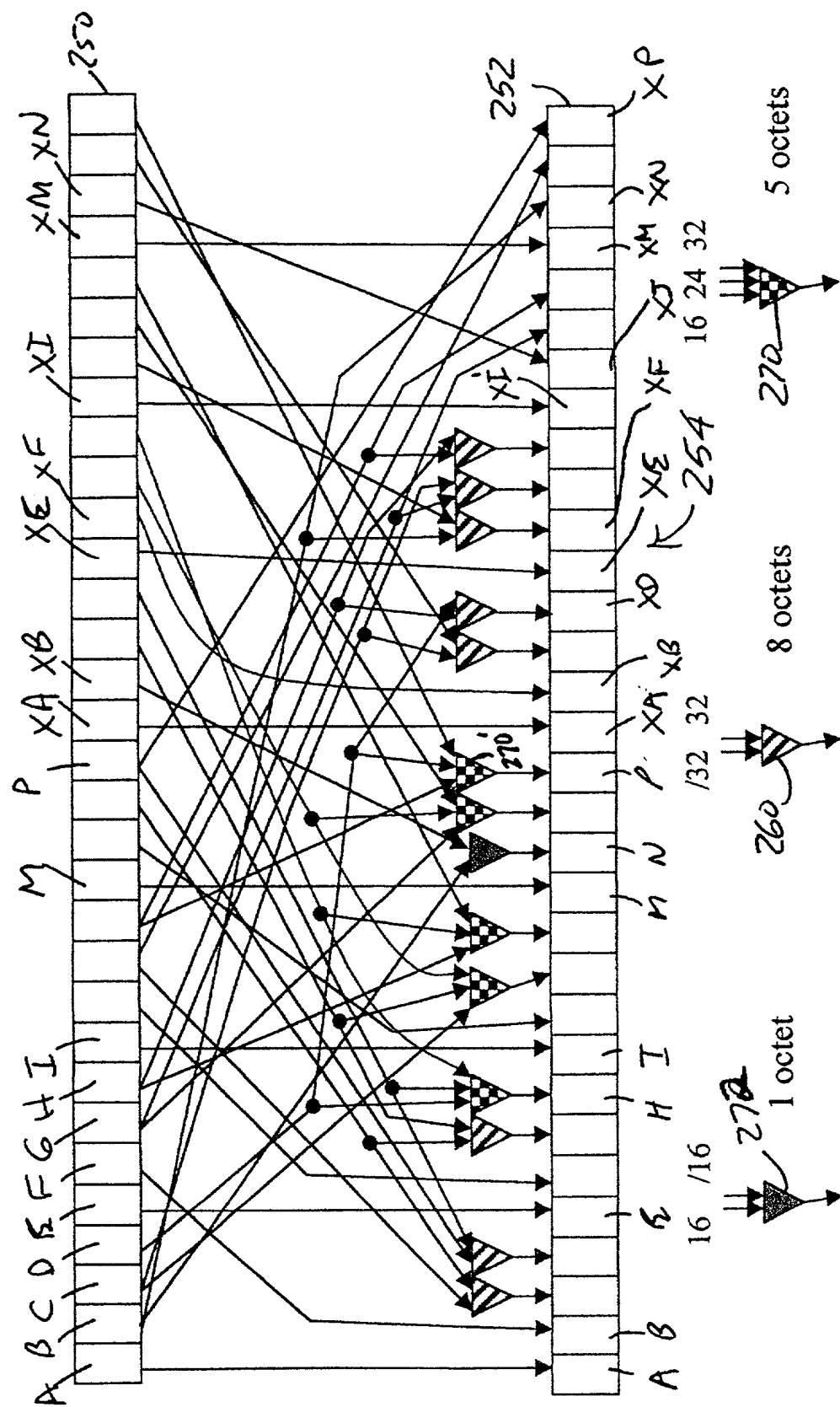


Fig. 10

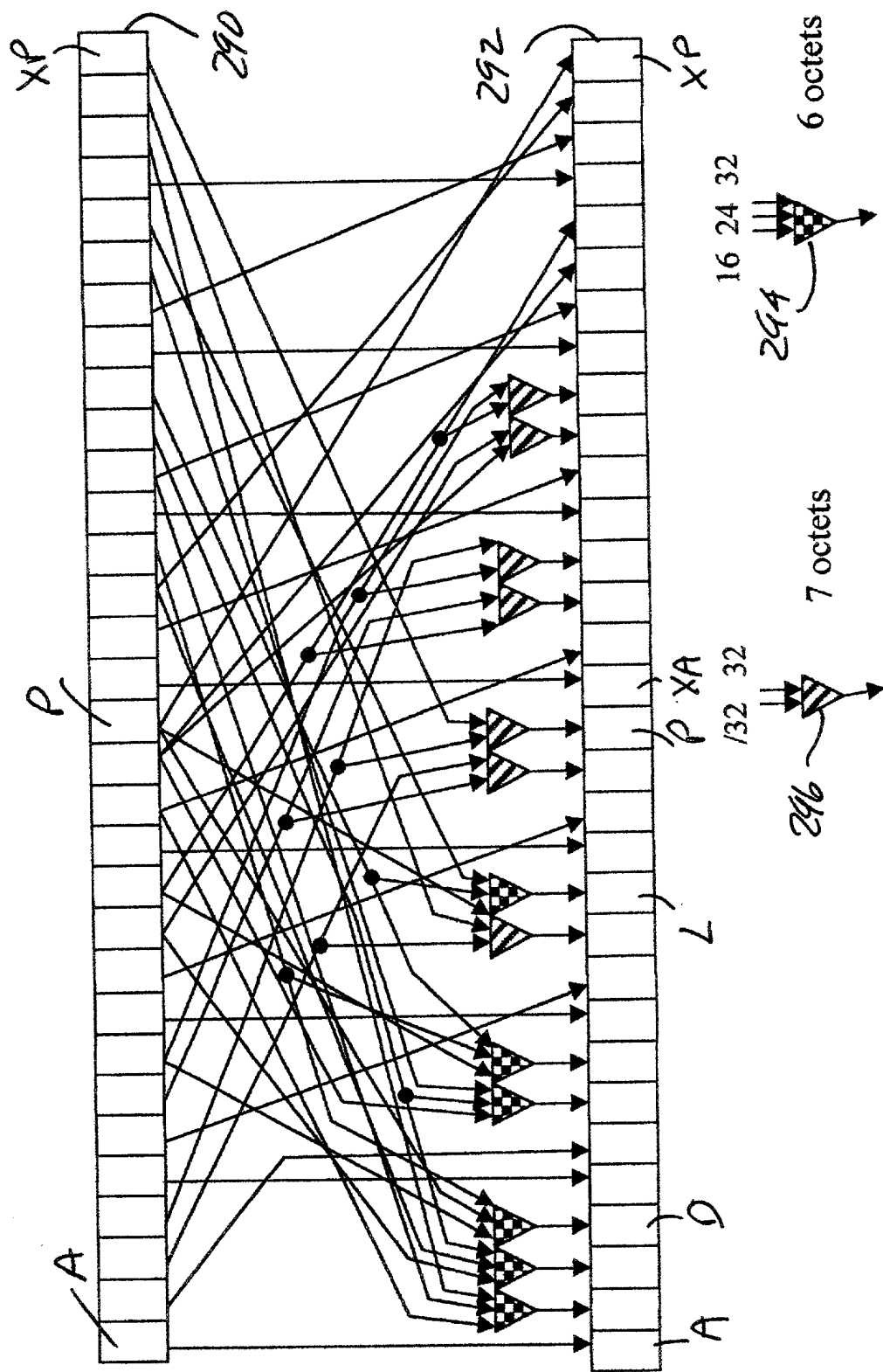


Fig. 11

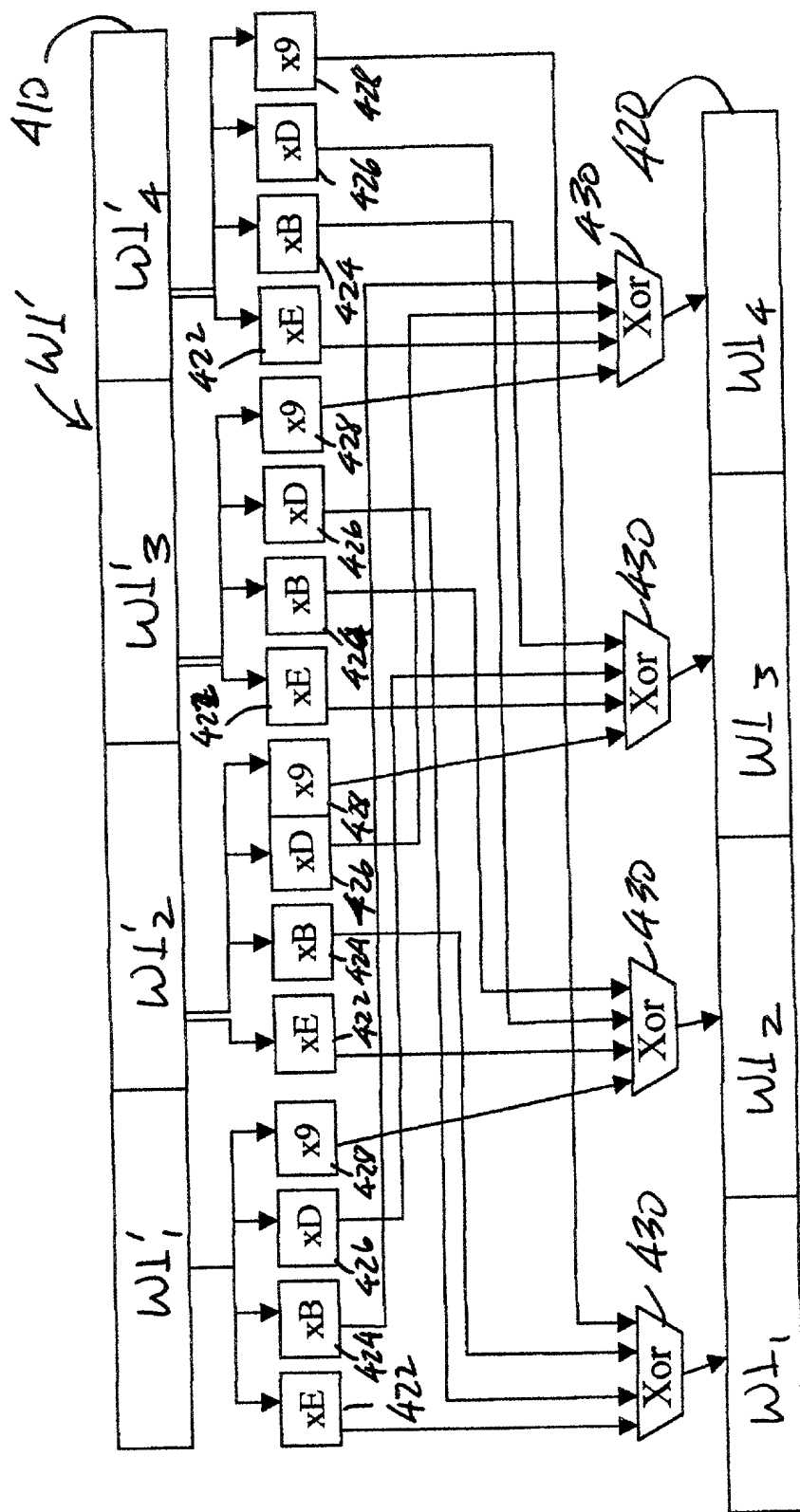
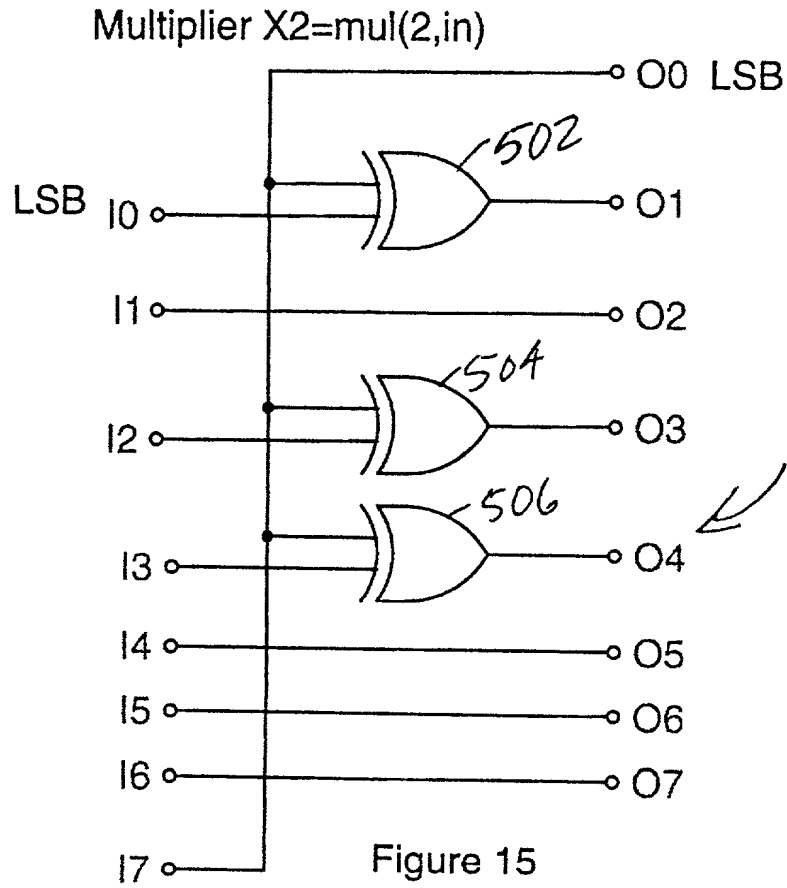


Fig. 14



365

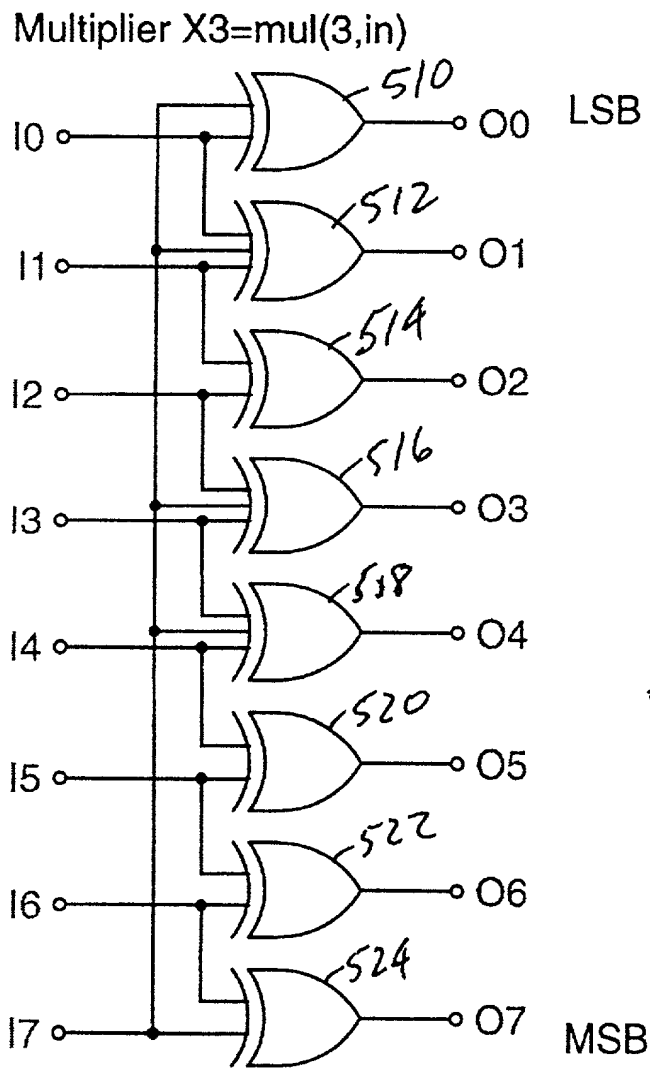


Figure 16

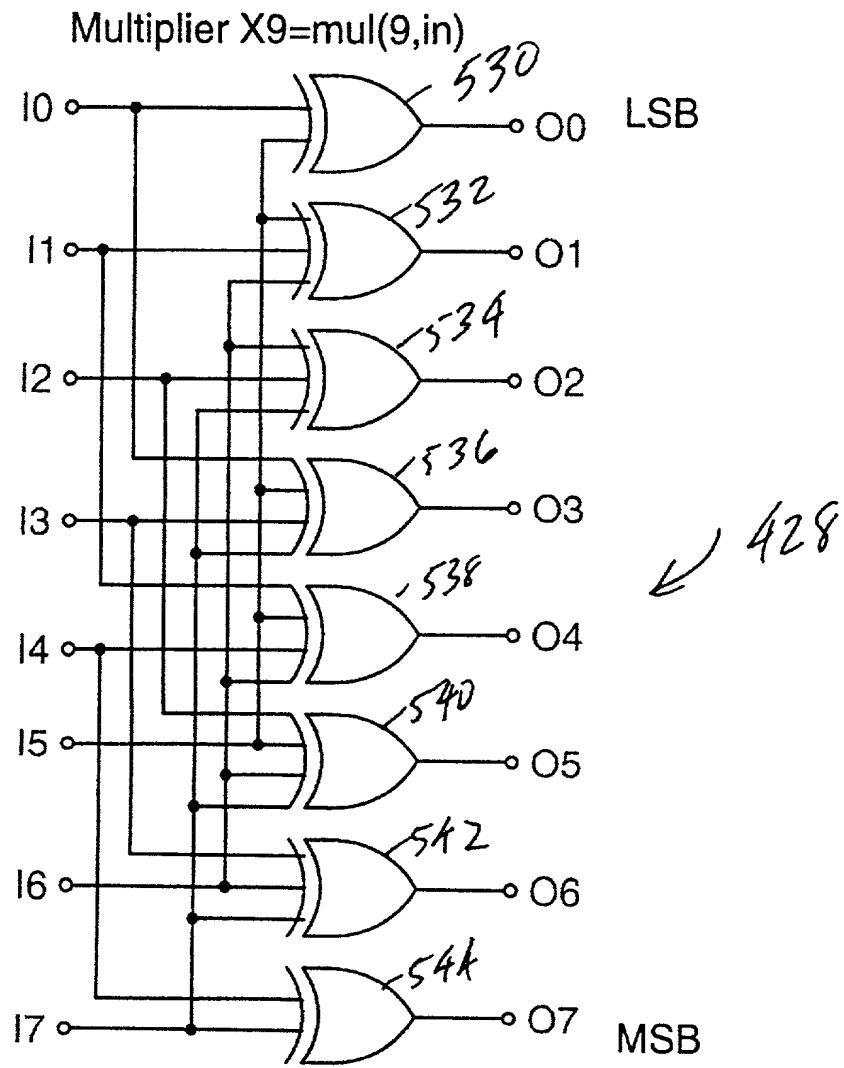


Figure 17

00000000 00000000 00000000 00000000

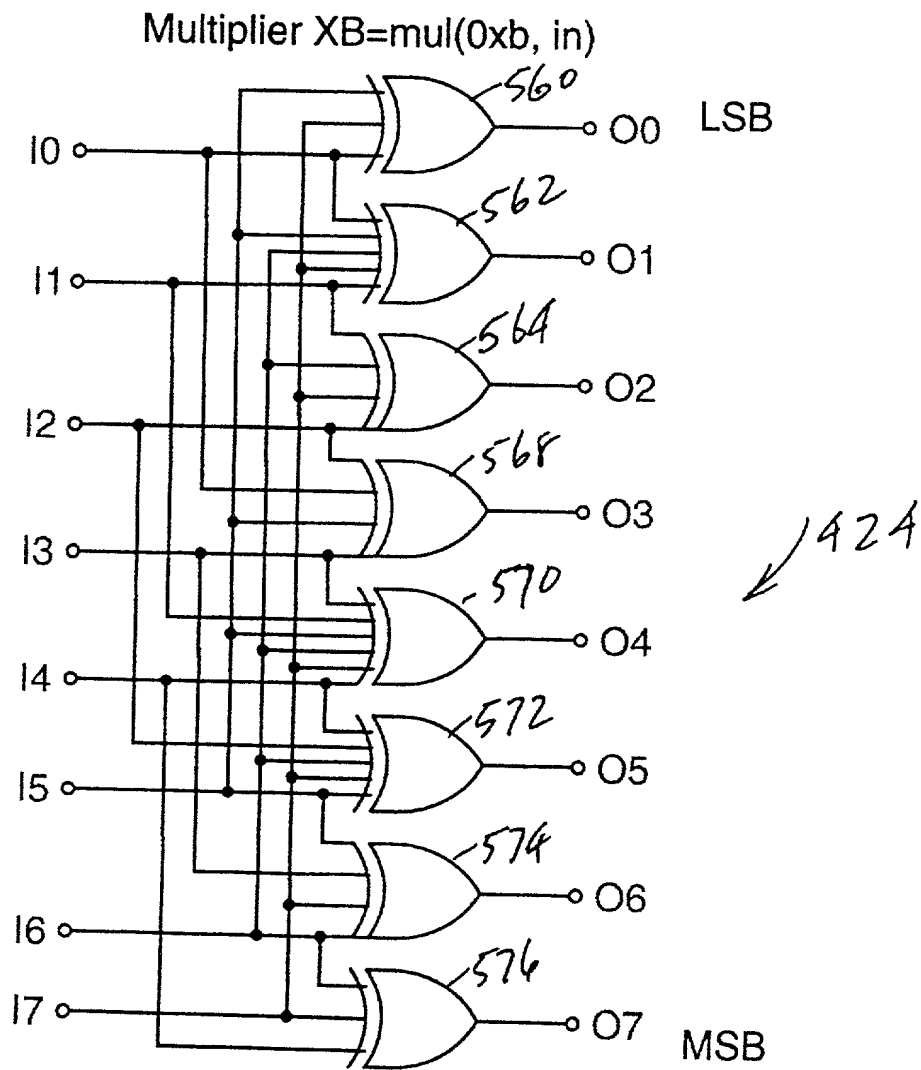


Figure 18

20140101 23004001

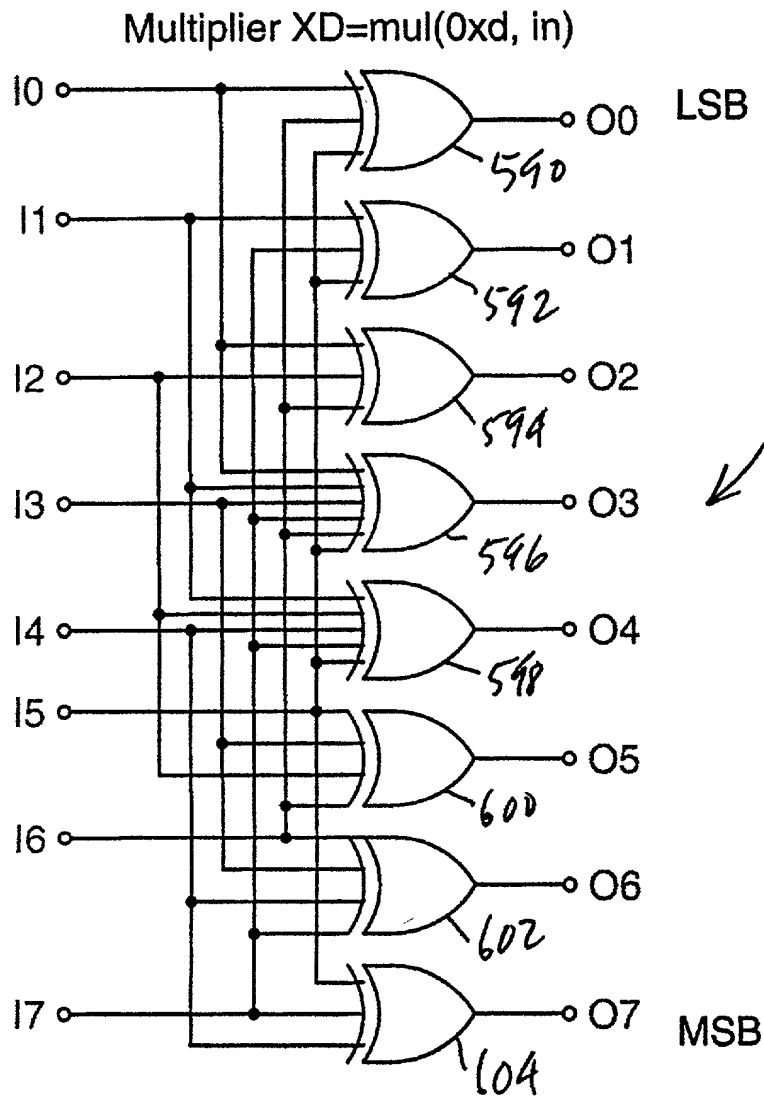


Figure 19

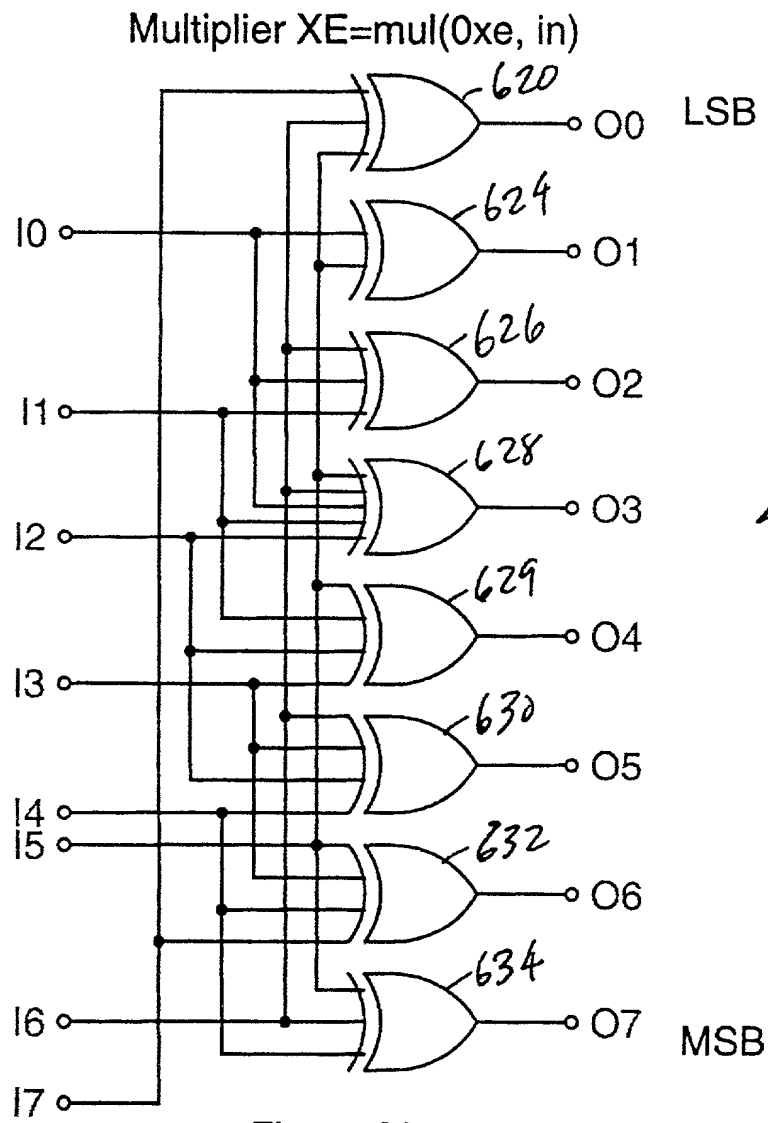


Figure 20

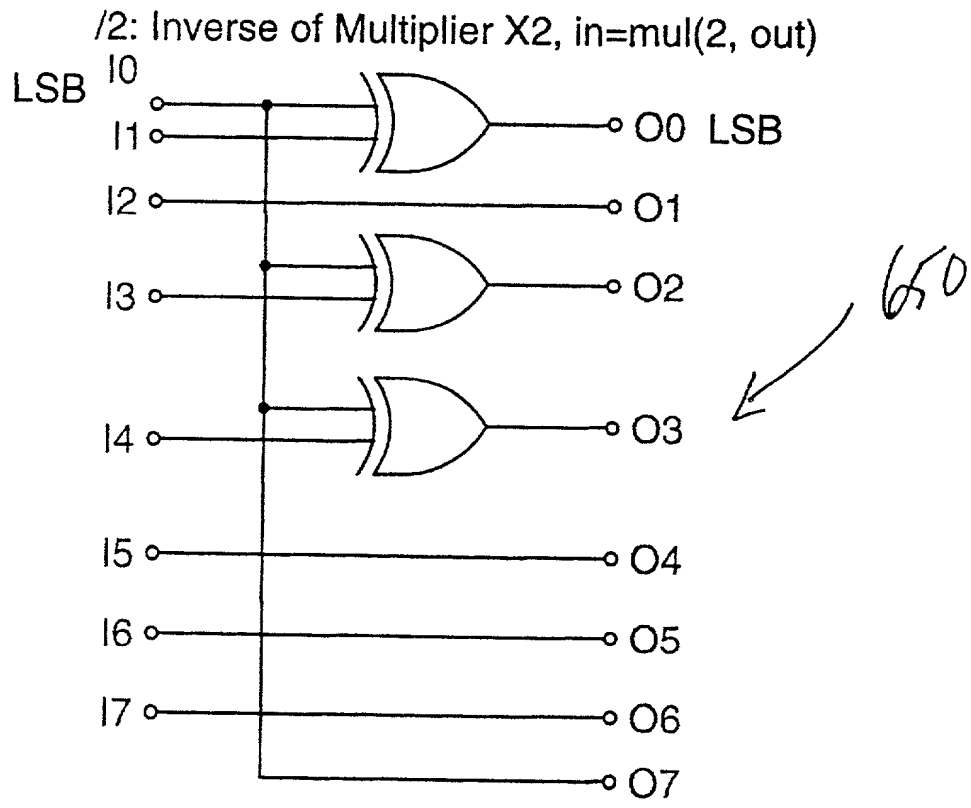


Figure 21

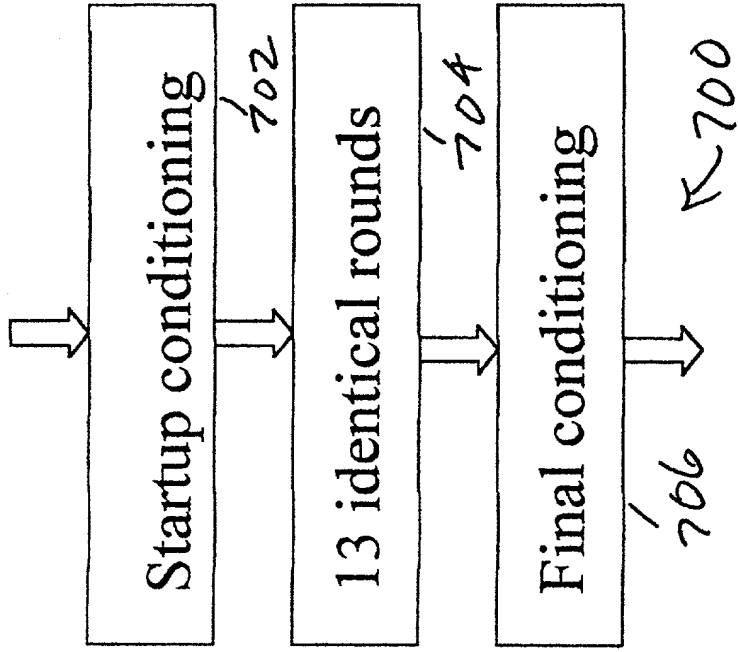


Fig. 22

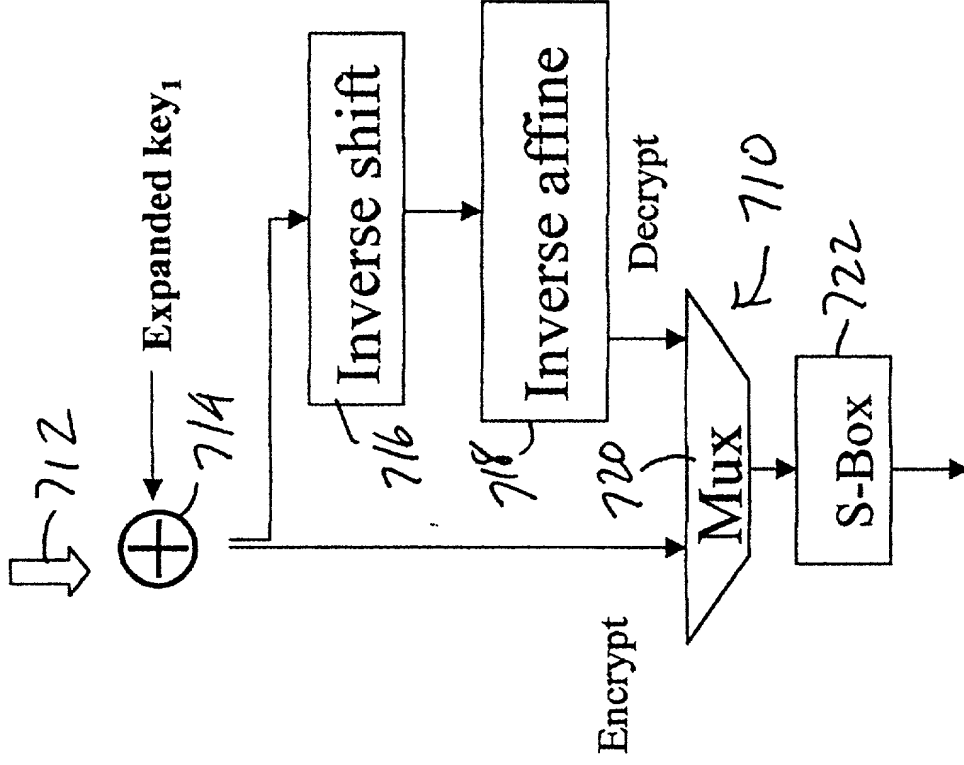


Fig. 23

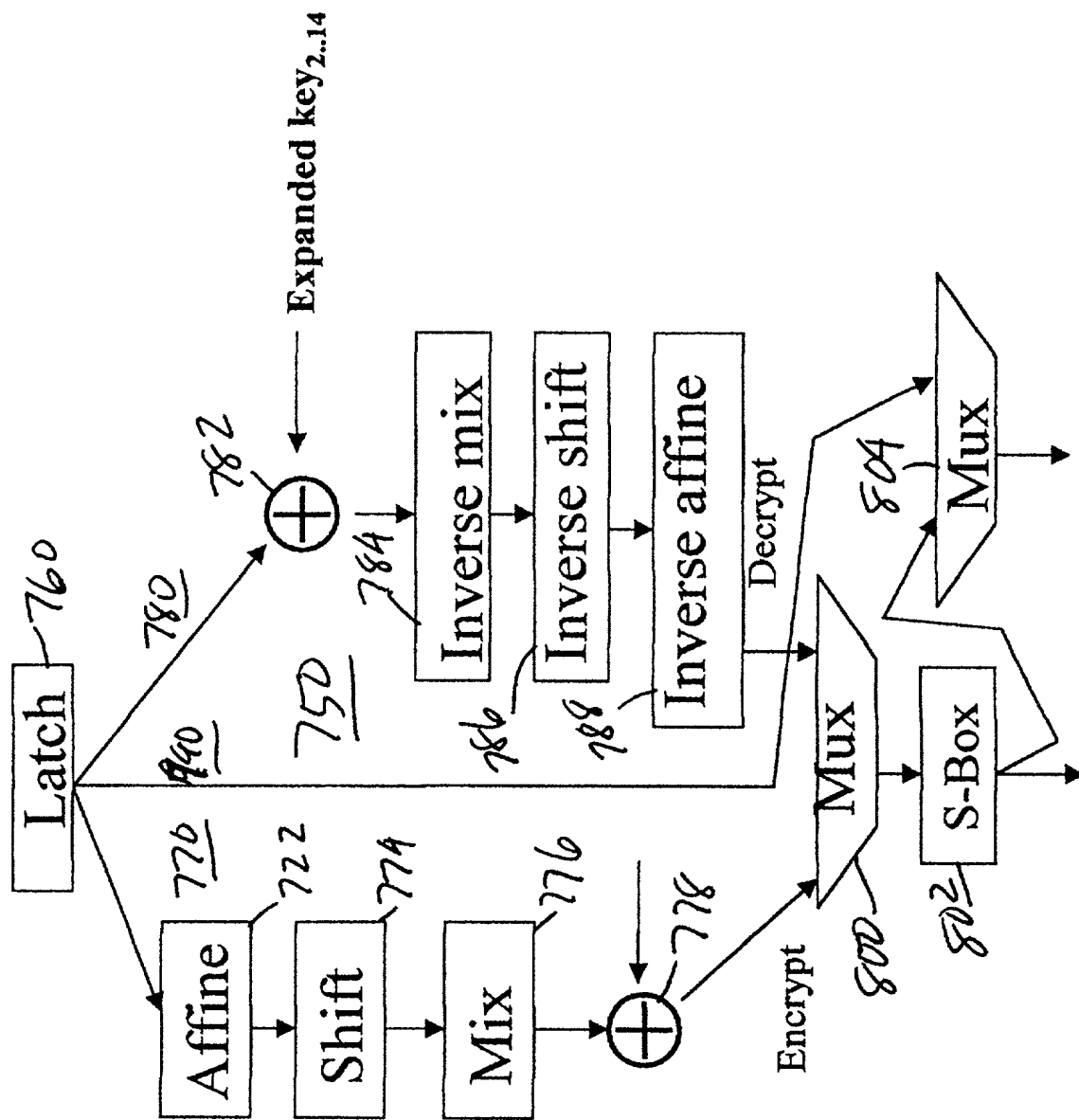


Fig. 24

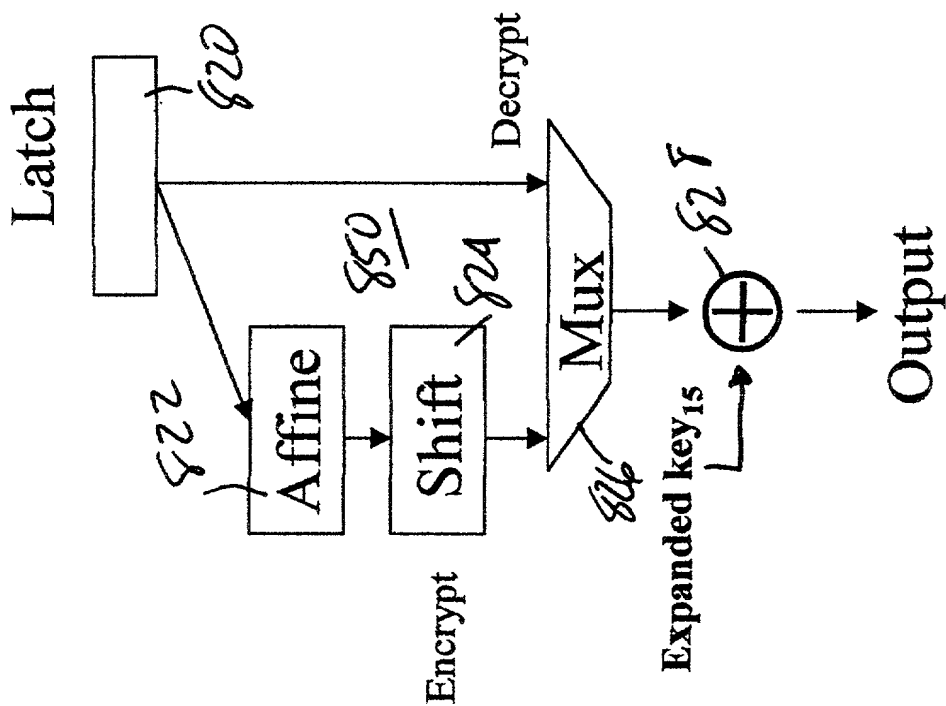


Fig. 25

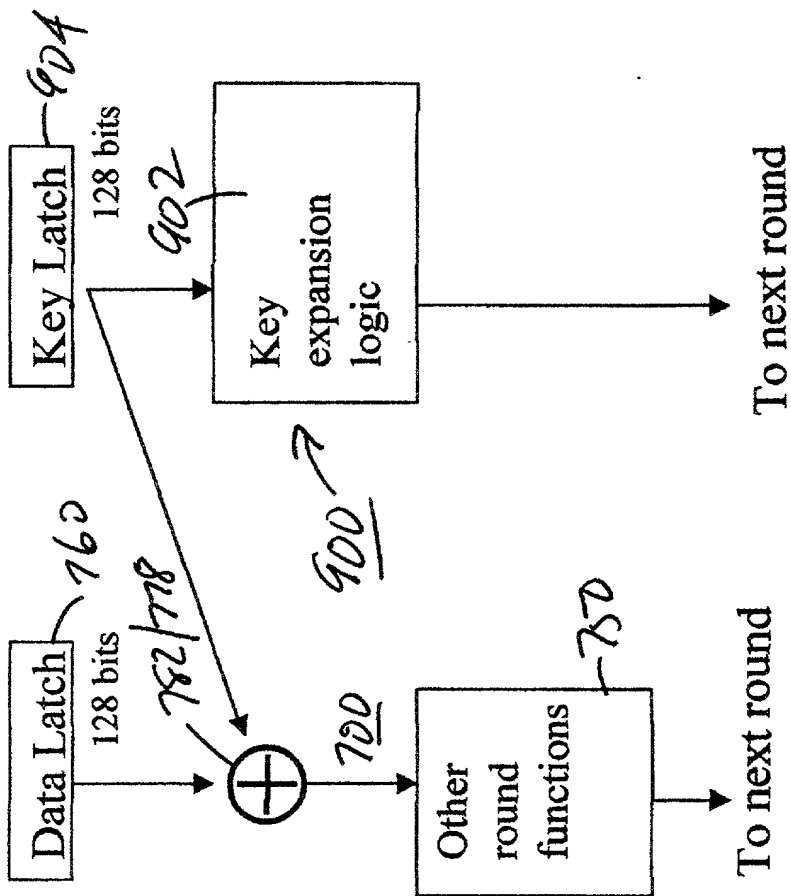
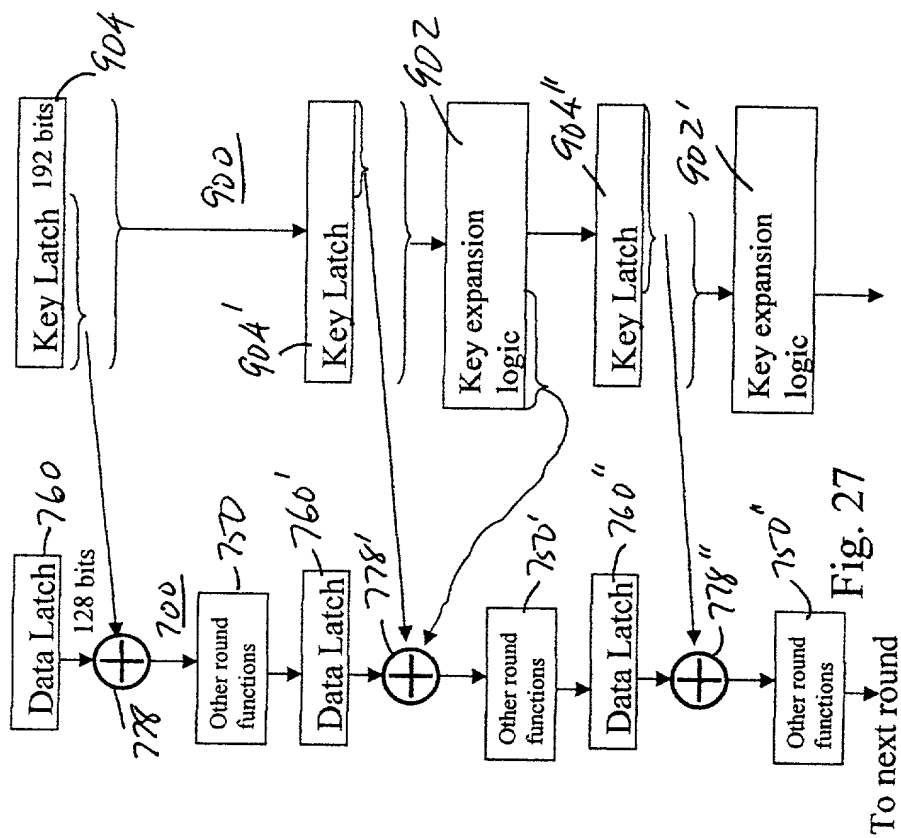


Fig. 26



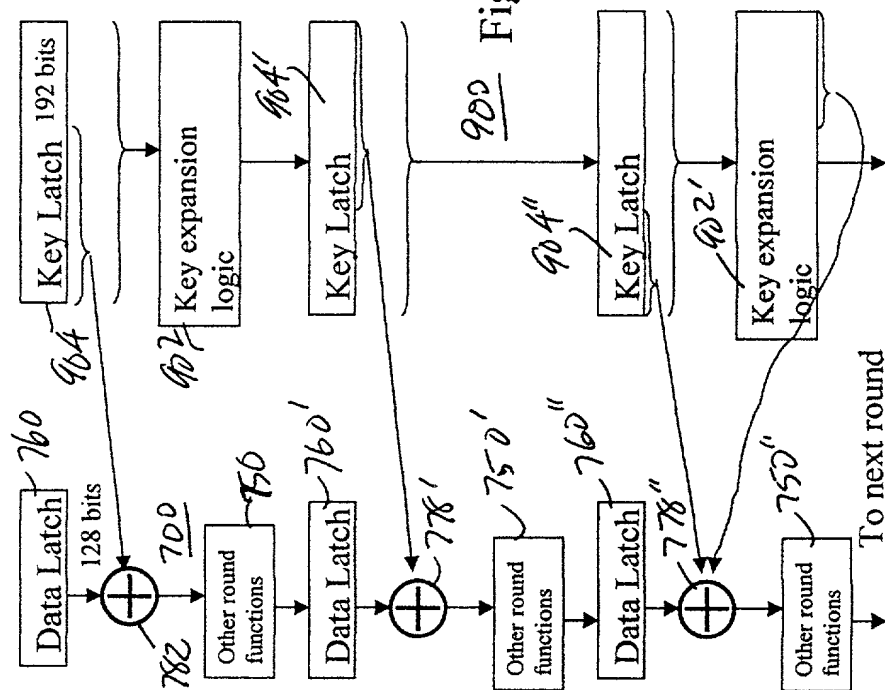


Fig. 28

20040101 25000000

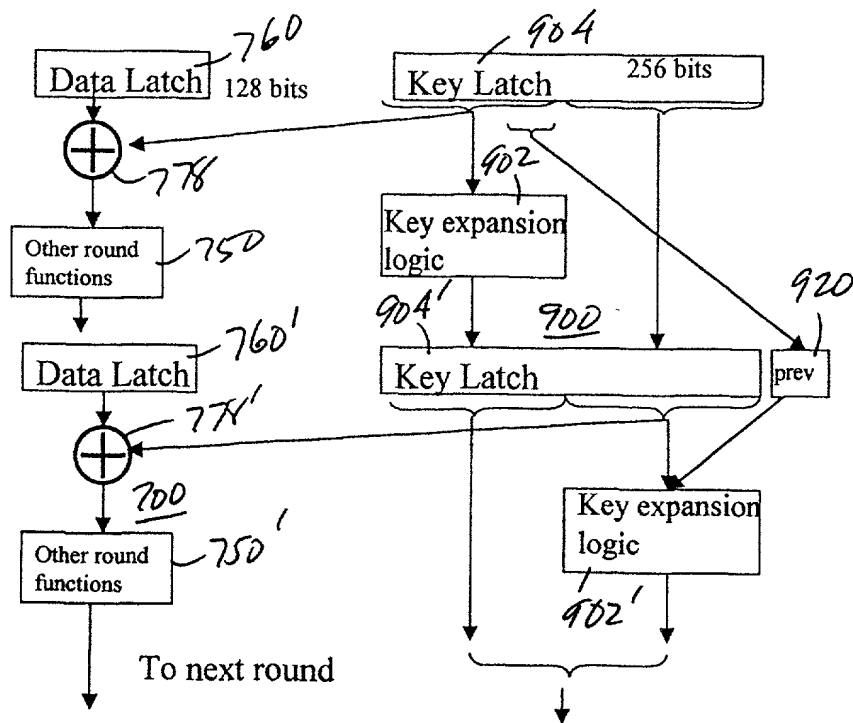
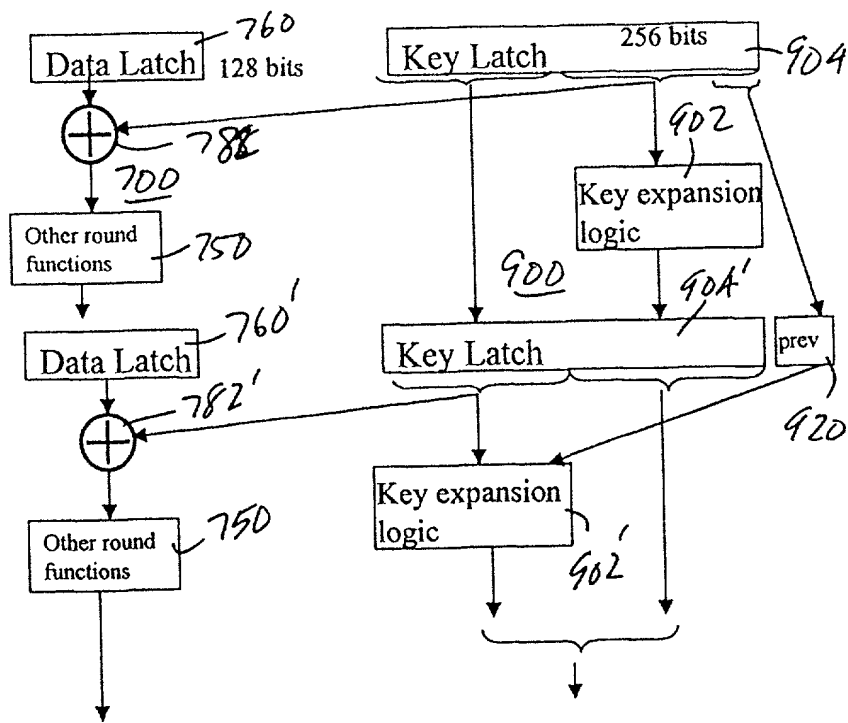


Fig. 29



To next round

Fig. 30

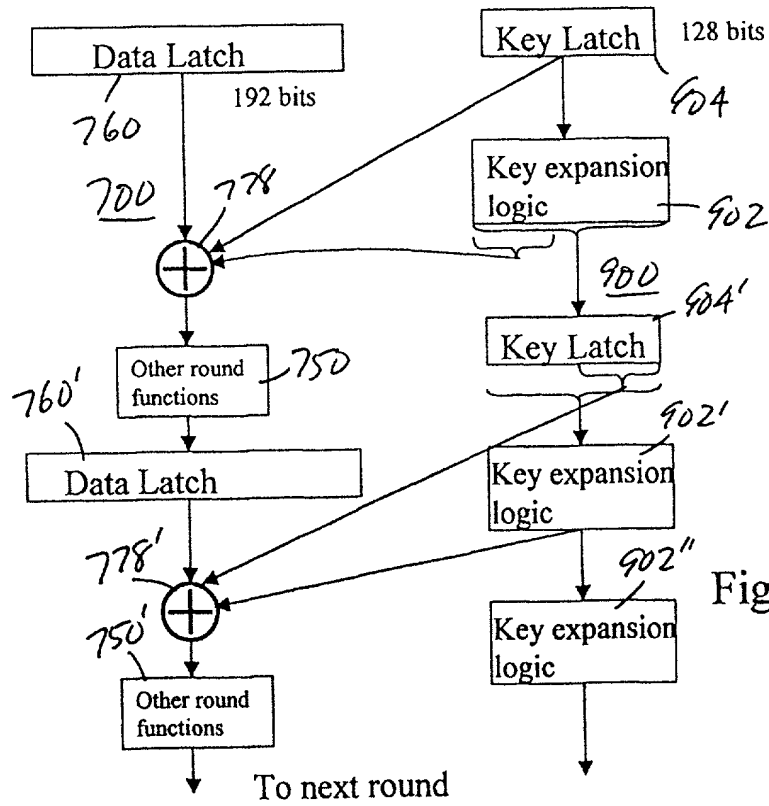


Fig. 31

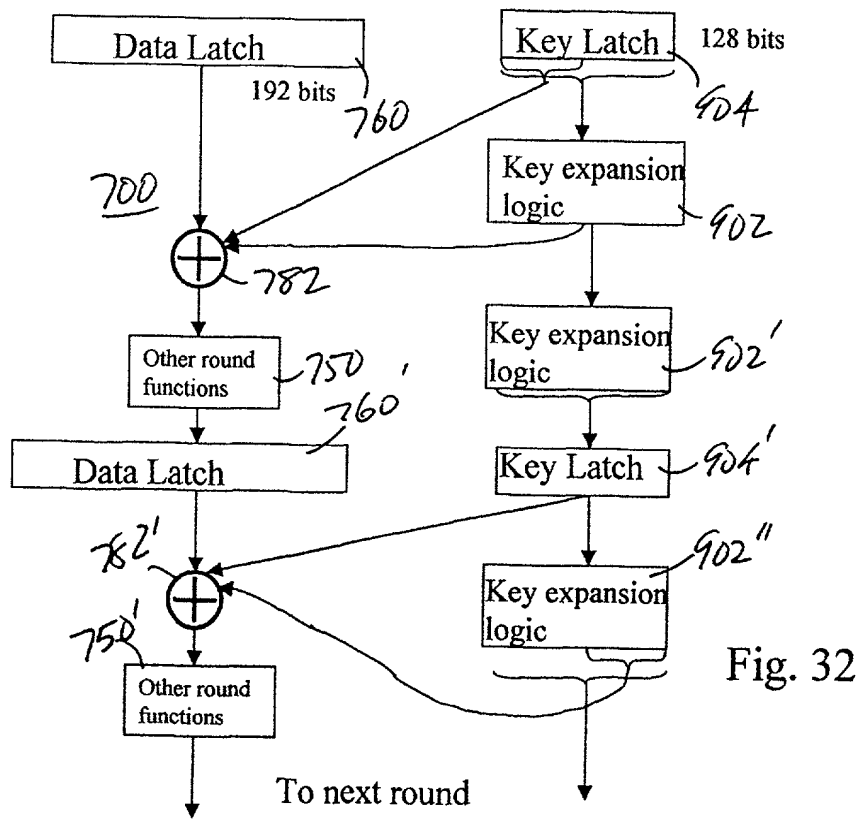


Fig. 32

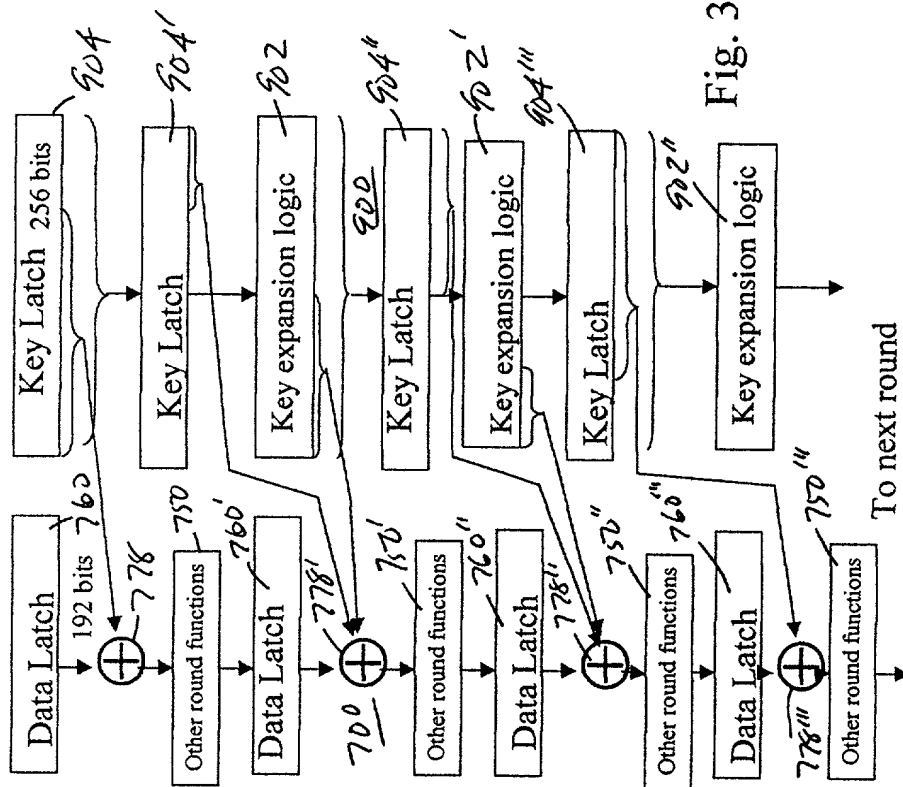


Fig. 34

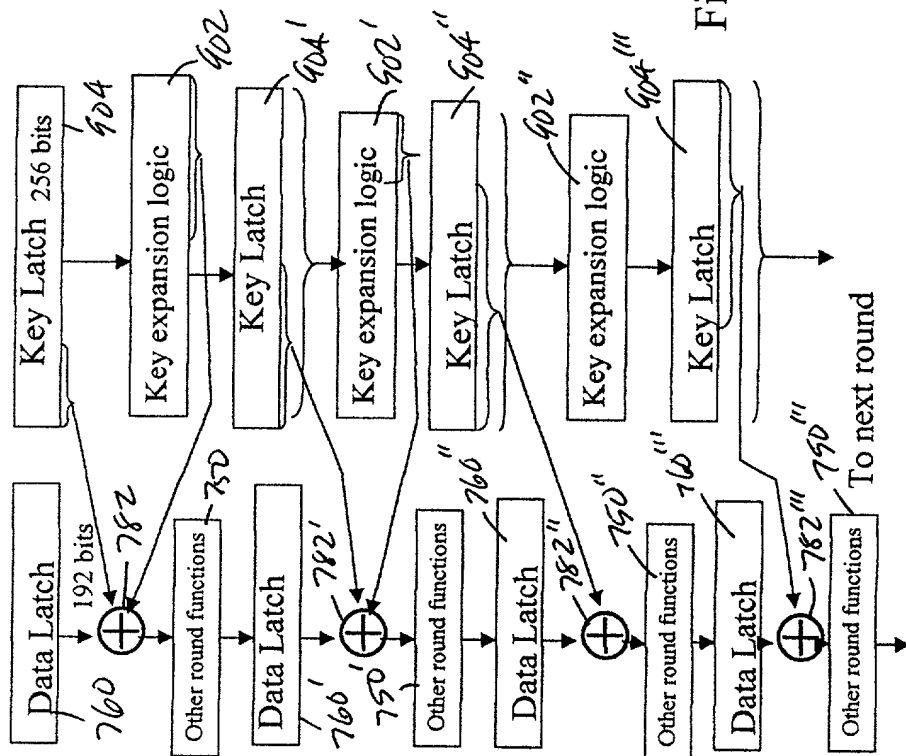


Fig. 35

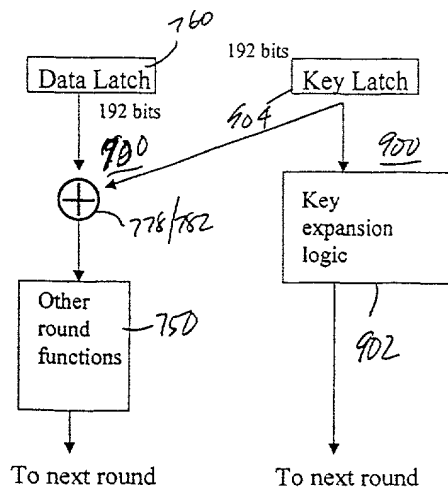


Fig. 33

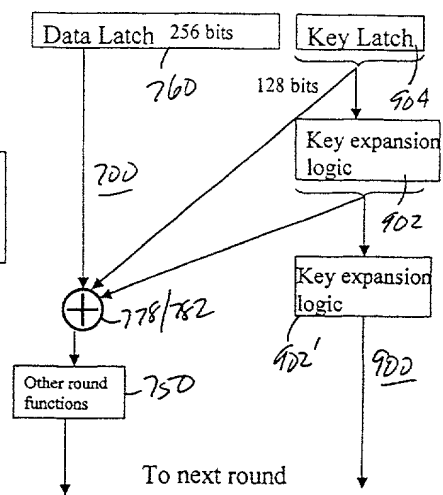
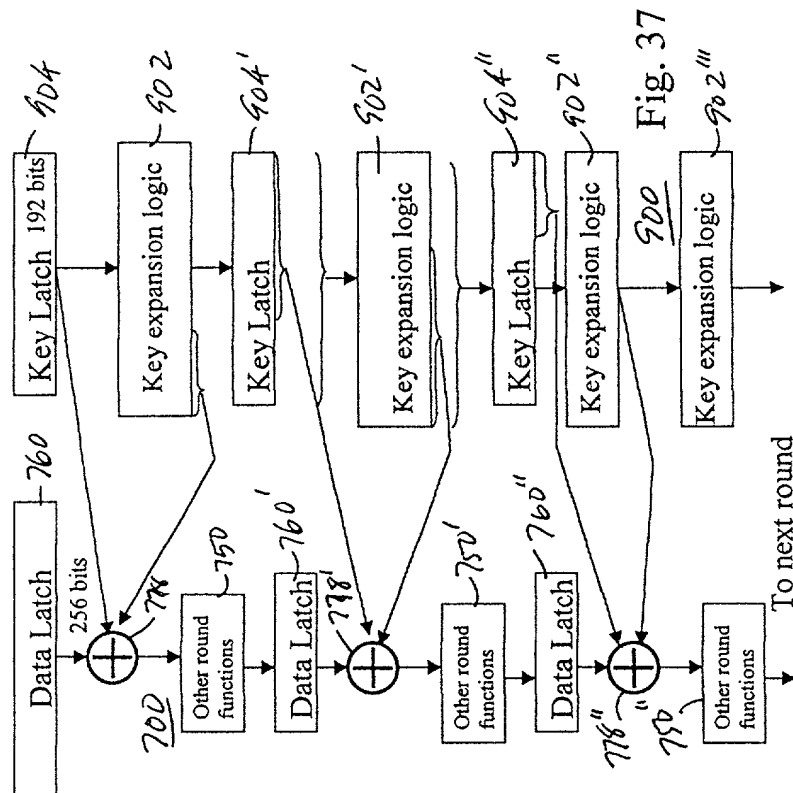
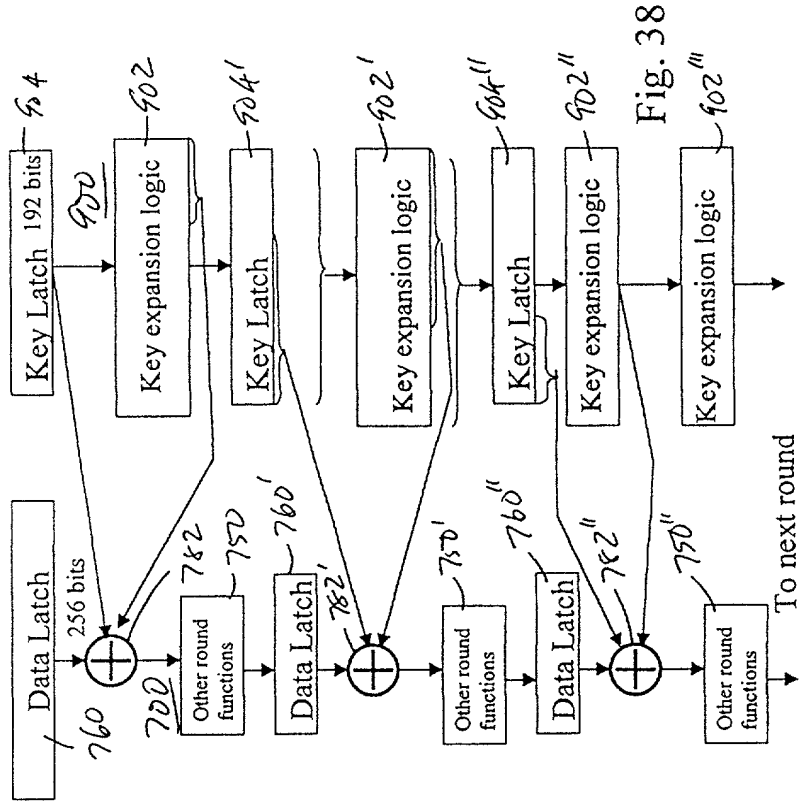


Fig. 36





Key expansion Logic

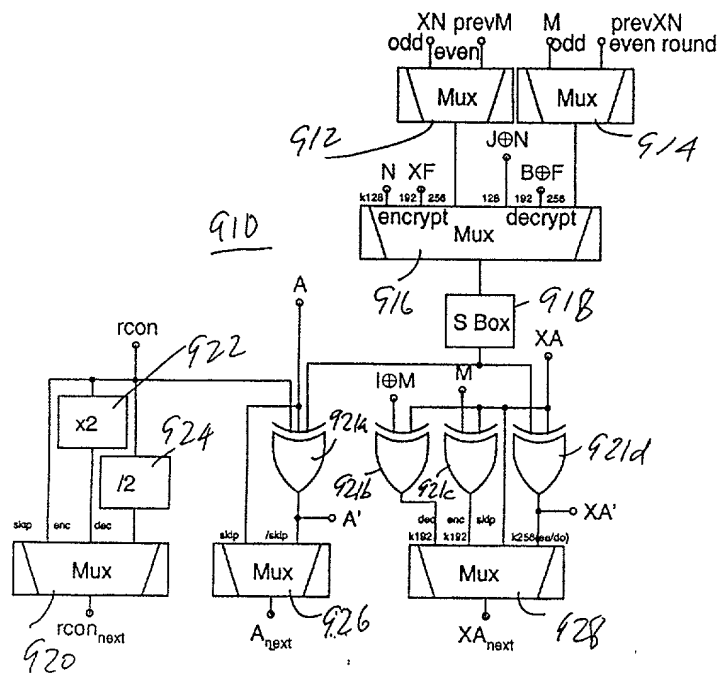
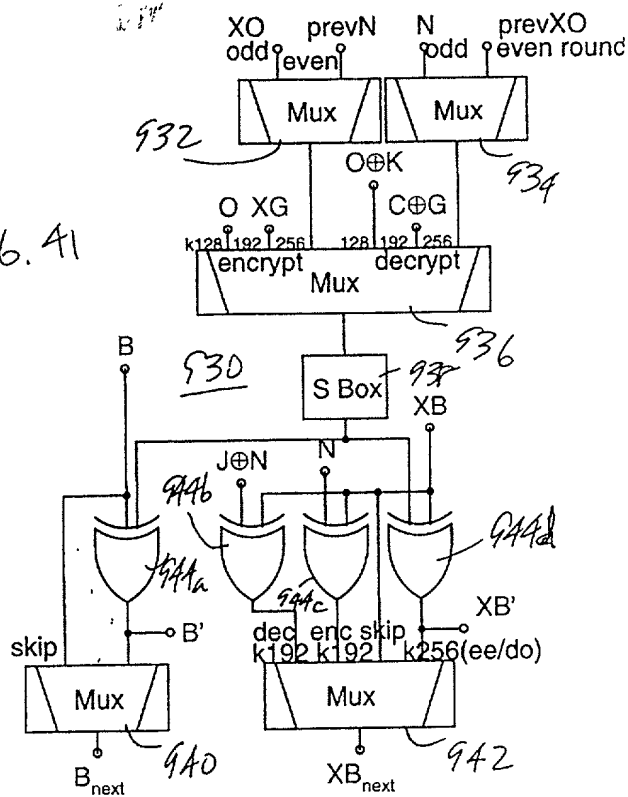


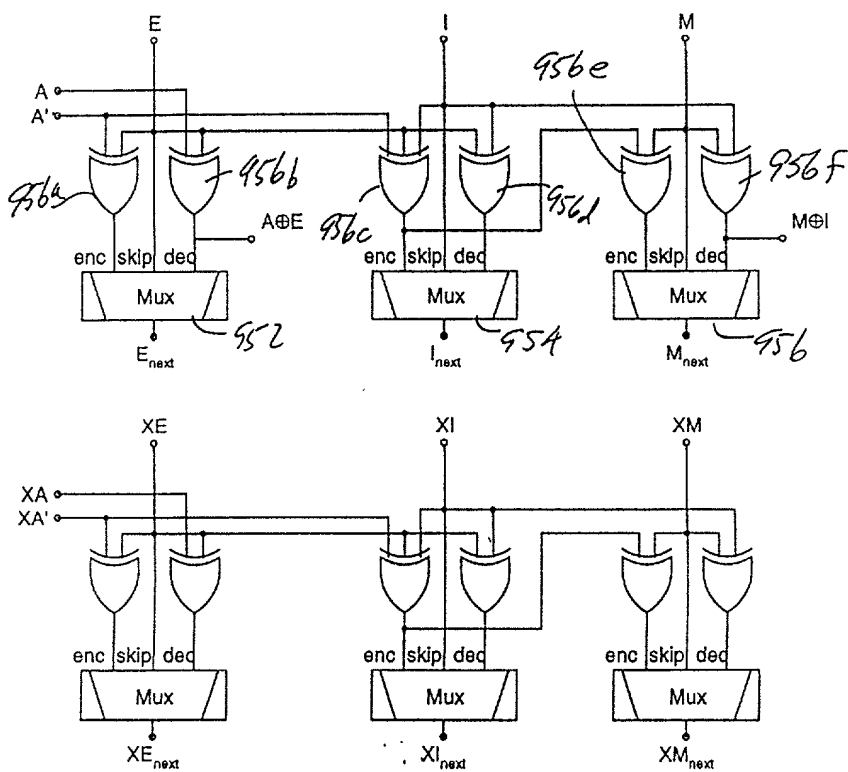
FIG. 4D

Key expansion Logic

FIG. 41

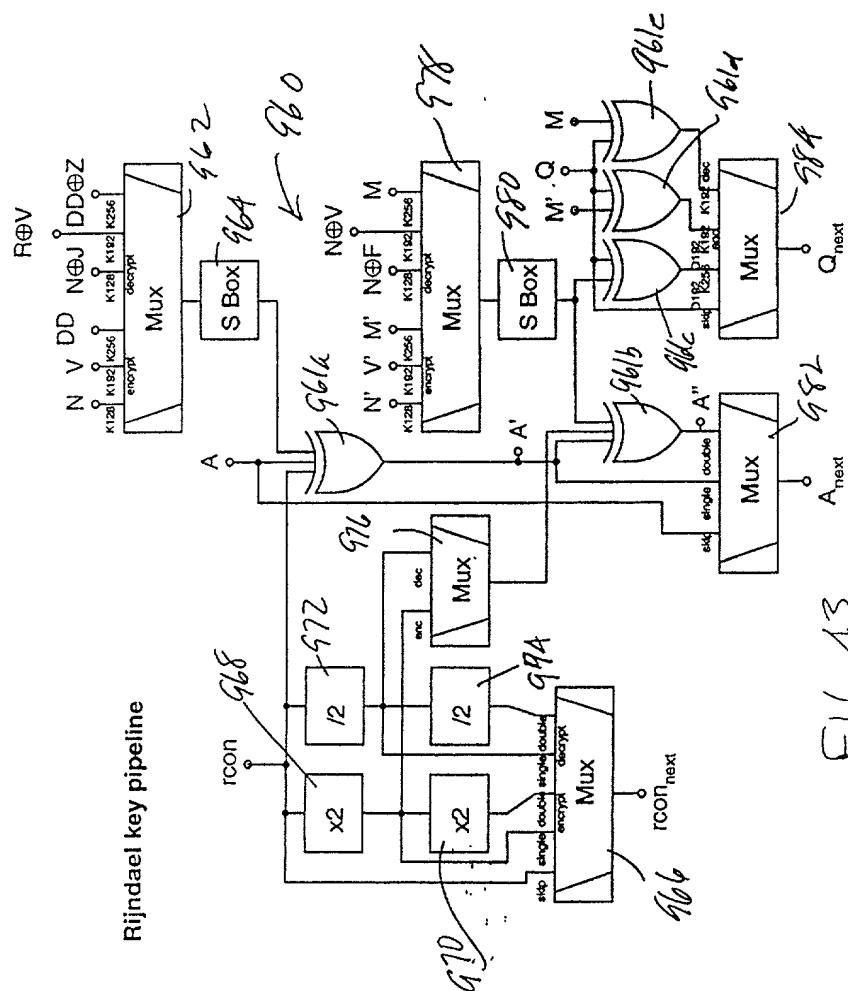


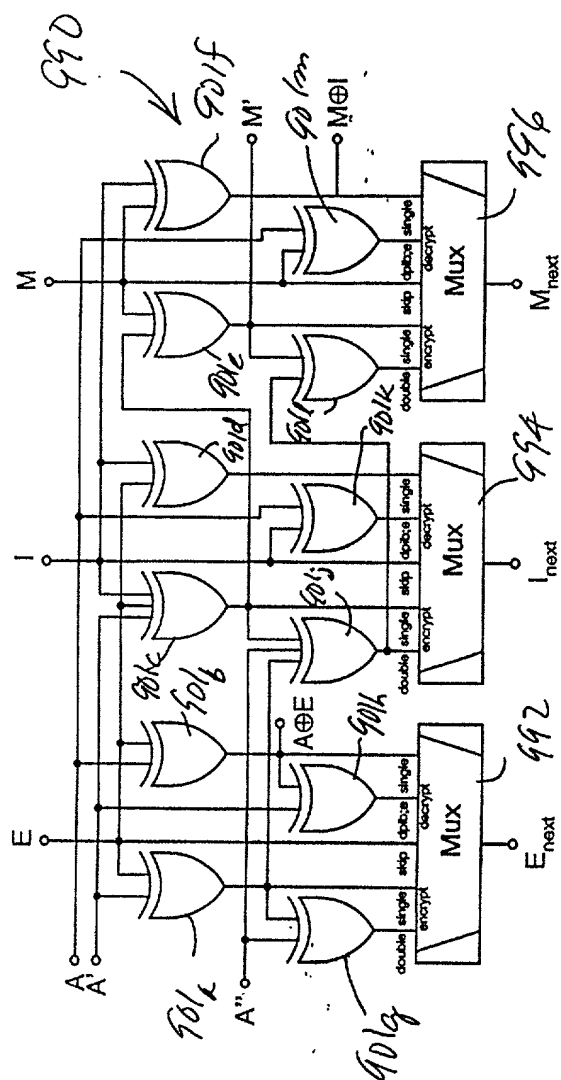
950



Key expansion Logic AES

F16.42





Rijndael Key Pipeline

F16.44

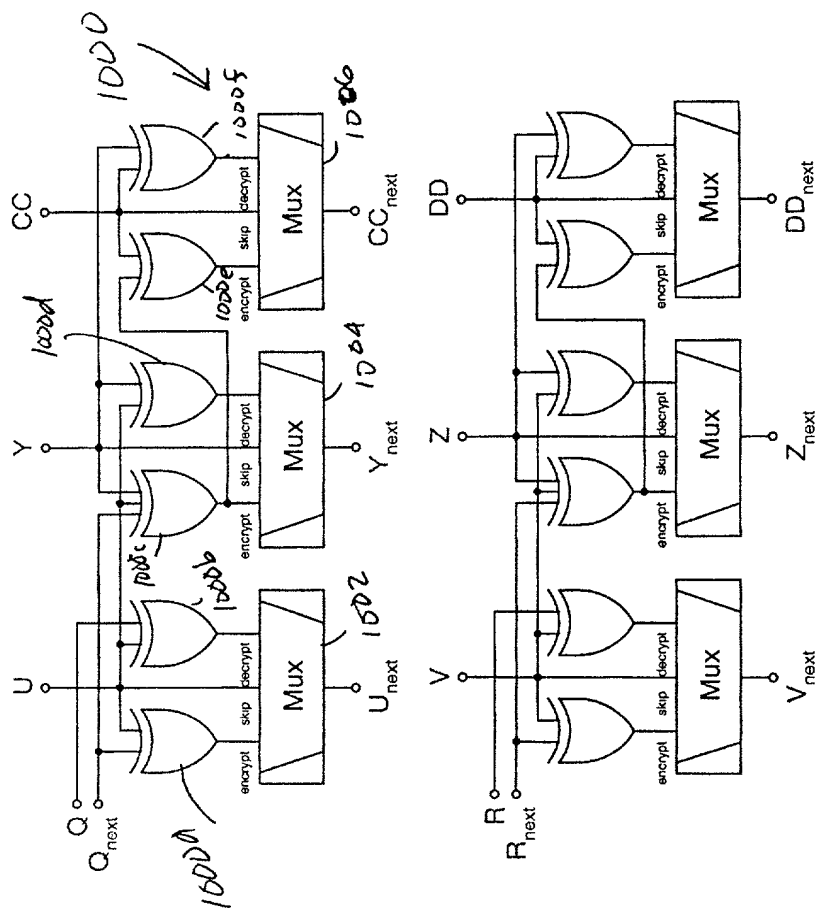


FIG. 45 Rijndael Key Pipeline